

FORTINET®

Sure, go hi-speed on the mobile with 3G, but beware the hacker

DECCAN Chronicle

April 15, 2011

Sure, go hi-speed on the mobile with 3G, but beware the hacker



April 11: Are those 200-200 ads tempting you to go 3G? Consider this before you do: Cybercriminals around the world are trying to steal data from your phone or even take control of it. And they have at least 2,200 types of malware, a number that's growing, to do the dirty job. What's worse, there's plenty of that happening close by - India is now said to be the third biggest originator of malware.

Vishak Raman, the regional director of security solutions company Fortinet, says these 2,200 malwares belong to some 200 different families of tools that cybercriminals use, and between them they are capable of attacking any mobile phone platform.

A 3G mobile phone could be attacked at four different levels - vulnerabilities on the device could be exploited, an application on the smartphone can be compromised, the peering gateways could be attacked when the mobile logs on to a roaming network, or it could be hit when you are browsing the Internet on the phone.

DEVICE: 3G devices work on special SIM cards, and in most cases, no one is sure what's been encrypted on these SIM cards. There could be loopholes that can be exploited by hackers trying to get hold of data on the

phone. APPS: A second vulnerability opens up when one downloads applications. Apps are the biggest draw on today's smartphones, and everybody wants loads of them. But apps, especially from sources other than the app stores of say an Apple or Google (Android), could well prove to be the horses that bring in the trojans.

PEERING GATEWAYS: A 3G smartphone's vulnerability to cybercrime attacks is very high at Peering Gateways when data passes between networks. When your phone moves from your native network in roaming mode into another network, the latter needs to copy the details of your device. While these two networks may be secure within themselves, vulnerabilities exist at the intersection, giving cybercriminals an opening to intercept your phone data when it's flowing between the networks.

BROWSING: While 3G phones allow you to browse the Internet just as you would on a desktop computer, they are also as vulnerable to online attacks through the browser as the PC is.

PHISHING: When Dileep, a Bengaluru-based cybersecurity professional, clicked on a link to download Yahoo Messenger onto

his 3G phone recently, the browser took him to a Website that said the download would cost him \$1. Dileep immediately knew this was a phishing website and did not attempt the download. Yahoo Messenger, after all, is available for free.

Had he continued with the process, though, Dileep would have been the victim of a cybercriminal. For, not only would he have paid for something that is free to download, he would have also given those behind the website his credit card details.

BB UNDER ATTACK: Anti-virus software maker Trend Micro says it has detected a Zeus trojan that is attacking BlackBerry users. Trend Micro country manager Amith Nath said the trojan is capable of blocking calls, deleting or forwarding SMS messages on a user's BlackBerry to the hacker without the user's knowledge. What's worse, it can even set up a new administrator, which means the hacker can take control of the phone.

Variants of the Zeus Trojan have been previously detected for the Symbian and Windows Mobile operating systems. They monitor users' private information, in particular when the user conducts mobile online banking.

US shuts down cyber theft ring

Washington, April 14: US authorities claimed one of their biggest victories against cyber crime as they shut down a ring they said used malicious software to take control of more than 2 million PCs around the world, and may have led to theft of over \$100 million.

A computer virus, dubbed Coreflood, infected more than 2 million PCs, enslaving them into a "botnet" that grabbed banking credentials and other data its masters used to steal funds via fraudulent banking and wire transactions, the US Justice Department said.

"This was big money stolen on a large scale by foreign criminals. The FBI wanted to stop it and they did an incredibly good job at it," said Alan Paller, director of research at the SANS Institute, a nonprofit group that helps fight cyber crime. The vast majority of the infected machines were in the United States, but the criminal gang was likely overseas.

"We're pretty sure a Russian crime group was behind it," said Paller. Paller and other security experts said it was hard to know how much money the gang stole. It could easily be tens of millions of dollars and could go above \$100 million, said Dave Marcus, McAfee Labs research and communications director.

A civil complaint against 13 unnamed foreign nationals was also filed by the U.S. district attorney in Connecticut. It accused them of wire and bank fraud. The Justice Department said it had an ongoing criminal investigation.

The malicious Coreflood software was used to infect computers with keylogging software that stole user names, passwords, financial data and other information, the Justice

Department said. "The seizure of the Coreflood servers and Internet domain names is expected to prevent criminals from using Coreflood or computers infected by Coreflood for their nefarious purposes," U.S. Attorney David Fren said in a statement.

In March, law enforcement raids on servers used by a Rustock botnet were shut down after legal action against them by Microsoft Corp. Authorities severed the Rustock IP addresses, effectively disabling the botnet.

Rustock had been one of the biggest producers of spam e-mail, with some tech security experts estimating they produced half the spam that fills people's junk mail bins.

A botnet is essentially one or more servers that spread malicious software and use the software to send spam or to steal personal information or data that can be used to empty a victim's bank account.

US government programmers shut down the Coreflood botnet on Tuesday. They also instructed the computers enslaved in the botnet to stop sending stolen data and to shut down. A similar tactic was used in a Dutch case, but it was the first time US authorities had used this

method to shut down a botnet, according to court documents. Victims of the botnet included a real estate company in Michigan that lost \$115,771, a South Carolina law firm that lost \$78,421 and a Tennessee defense contractor that lost \$24,866, according to the complaint filed in the U.S. District Court for the District of Connecticut.

The government plans to work with Internet service providers around the country to identify other victims. — Reuters